ACADEMIC PRESS

Available at WWW.MATHEMATICSWEB.ORG POWERED BY SCIENCE DIRECT®

Journal of Number Theory 101 (2003) 270–293

JOURNAL OF Number Theory

http://www.elsevier.com/locate/jnt

Local units and Gauss sums

Miho Aoki*

Department of Mathematics, Tokyo Metropolitan University, 1-1 Minami-Ohsawa, Hachioji-shi, Tokyo-to, 192-0397, Japan

Received 17 May 2002; revised 7 January 2003

Communicated by D. Goss

Abstract

In this paper, we will determine the structure of a certain module which is related to the plus part of the ideal class groups in terms of the divisibility of Gauss sums in some local fields. This result is a generalization of a result of Iwasawa and the previous work of Ichimura and Hachimori.

MSC: 11R23

Keywords: Gauss sums; Euler system

1. Introduction

Let F be an abelian number field. Fix an odd rational prime p and let F_∞ denote the cyclotomic $\mathbb{Z}_p$-extension of F. We have a sequence of fields

$$F = F_0 \subset F_1 \subset \cdots \subset F_m \subset \cdots \subset F_\infty$$

such that F_m/F is a cyclic extension of degree p^m.

For any number field K, let A_K be the p-primary component of the ideal class group of K, and set $X = \varprojlim A_{F_m}$. By the action of complex conjugation, X is decomposed to $X^+ \oplus X^-$. Fix a topological generator γ of $\Gamma = \mathrm{Gal}(F_\infty/F)$.

*Fax: +81-426-77-2472.

E-mail address: maoki@comp.metro-u.ac.jp.

0022-314X/03/$ - see front matter
doi:10.1016/S0022-314X(03)00056-8

Suppose first $F = \mathbb{Q}(\mu_p)$, where μ_p is the group of all pth roots of unity. Kolyvagin [6] and Rubin [9] determined the structure of $(X^-)_\Gamma = X^-/(\gamma - 1)X^- \simeq A_F^-$ as an abelian group (Theorem 1). The structure is determined by certain elements obtained from Stickelberger elements. For the proof, they used the Euler system of Gauss sums. One of the keys of the proof is to know the maximum n such that certain elements constructed from the Gauss sums belong to $(F^\times)^{p^n}$.

On the other hand, the local properties of Gauss sums (namely, the properties of Gauss sums in the completion of F for a prime ideal above p) give information on the plus part X^+. Iwasawa [5] gave a condition for $X^+ = 0$ (this is equivalent to the conjecture of Vandiver) by using the local properties of Gauss sums.

Let $\kappa : \Gamma \to \mathbb{Z}_p^\times$ be the cyclotomic character. In this paper, we will determine the structure of $X^+/(\gamma - \kappa(\gamma))X^+$ by using Gauss sums for an abelian number field F satisfying certain conditions. Note that if $F = \mathbb{Q}(\mu_p)$, then the p-rank of $X^+/(\gamma - \kappa(\gamma))X^+$ (namely, $\dim_{\mathbb{Z}/p}(X^+/(\gamma - \kappa(\gamma))X^+ \otimes_{\mathbb{Z}} \mathbb{Z}/p)$) is the same as that of $X^+/(\gamma - 1)X^+ \simeq A_F^+$. For the proof, we will use local properties of the Euler system of Gauss sums, and also use some properties on the Euler system of Gauss sums proved by Kolyvagin and Rubin.

Let Δ be a finite abelian group and $\psi : \Delta \to \overline{\mathbb{Q}_p}^\times$ be a character. Let $\mathcal{O}_\psi$ denote the extension ring of $\mathbb{Z}_p$ which is generated by the values of ψ, and $\underline{\mathcal{O}_\psi}$ be the Δ-module which is $\mathcal{O}_\psi$ as an additive group on which Δ acts via ψ. We define the idempotent e_ψ by $e_\psi = \frac{1}{|\Delta|}\sum_{\sigma\in\Delta} \mathrm{Trace}(\psi^{-1}(\sigma))\sigma$, where $\mathrm{Trace} : \mathbb{Q}_p(\psi(\sigma)|\sigma\in\Delta) \to \mathbb{Q}_p$ is the trace map.

For any $\mathbb{Z}_p[\Delta]$-module Y, we define the ψ-part Y_ψ of Y by

$$Y_\psi = Y \otimes_{\mathbb{Z}_p[\Delta]} \underline{\mathcal{O}_\psi}.$$

Fix an odd character χ of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ which is not the Teichmüller character ω. Here, we assume the following two assumptions on χ:

(1) the order of χ is finite and prime-to-p.
(2) $\chi(p) \neq 1$ and $\omega\chi^{-1}(p) \neq 1$.

Let F_χ be the fixed field of the kernel of χ, and let $F = F_\chi(\mu_p)$. Set $\Delta = \mathrm{Gal}(F/\mathbb{Q})$. By assumption (1), the order of Δ is prime to p, and for any $\mathbb{Z}_p[\Delta]$-module Y, we have

$$Y_\psi \simeq e_\psi Y \quad \text{and} \quad Y = \bigoplus_\psi Y_\psi,$$

where ψ runs over all representatives of $\mathbb{Q}_p$-conjugate classes of characters of Δ. For an element a in Y, we denote the image of a in Y_ψ by a_ψ.

Let M be a power of p such that $M \geqslant |A_{F,\chi}|^2$. For any integer $i \geqslant 0$, let

$$\mathsf{S}_i = \{n \in \mathbb{Z} > 0 \mid \text{square-free, } n = \ell_1 \cdots \ell_i (\text{product of primes}),$$

$$\ell_j \equiv 1 \pmod{MN_F}\}$$

where N_F is the conductor of F. Let $\mathsf{S} = \bigcup_{i\geqslant 0} \mathsf{S}_i$. As mentioned before, Rubin determined the structure of $X_\chi/(\gamma-1)X_\chi \simeq A_{F,\chi}$ in terms of certain elements $d(n)$, $n\in\mathsf{S}$ which are obtained from Stickelberger elements (see Section 3.2 for the definition). Especially $d = d(1)$ is given the largest power of p dividing the generalized Bernoulli number $B_{1,\chi^{-1}}$.

Theorem 1 (Kolyvagin [6, Theorem 7], Rubin [9, Theorem 4.4]). *Write*

$$X_\chi/(\gamma-1)X_\chi(\simeq A_{F,\chi}) = \bigoplus_{i=1}^{t} \mathcal{O}_\chi/p^{e_i}, \quad e_1\geqslant\cdots\geqslant e_t$$

as $\mathcal{O}_\chi$-modules. Then we have

$$p^{e_{i+1}+\cdots+e_t} = \min\{d(n)\mid n\in\mathsf{S}_i\},$$

for any i, $0\leqslant i\leqslant t-1$.

Our aim is to determine the structure of $X_{\omega\chi^{-1}}/(\gamma-\kappa(\gamma))X_{\omega\chi^{-1}}$ as an $\mathcal{O}_\chi$-module. For each $n\in\mathsf{S}$, let $T(n)$ denote the $\mathcal{O}_\chi$-submodule of $(F^\times\otimes_{\mathbb{Z}}\mathbb{Q}_p/\mathbb{Z}_p)_\chi$ which is generated by elements $(\tau_{\mathfrak{r}}\otimes 1/d)e_\chi$ where $\tau_{\mathfrak{r}}$ is a Gauss sum of a prime ideal $\mathfrak{r}$ of F dividing n.

Let $M_{\infty,n}/F_\infty$ be the Kummer extension given by

$$M_{\infty,n} = F_\infty(\{a^{1/p^m}\mid a\otimes 1/p^m\in T(n)\}).$$

For any prime ideal $\mathfrak{r}$ of F lying above a rational prime $r\equiv 1\,(\mathrm{mod}\, nN_F)$, we will show that $(\tau_{\mathfrak{r}}^{\bar{e}_\chi})^{d(n)/d}$ is an element of $M_{\infty,n}^\times$ (Lemma 9), here, for any element $x\in\mathbb{Z}_p[\Delta]$, $\bar{x}$ denotes an element of $\mathbb{Z}[\Delta]$ satisfying $\bar{x}\equiv x\,(\mathrm{mod}\, d)$. Set $\beta_{\mathfrak{r},n} = (\tau_{\mathfrak{r}}^{\bar{e}_\chi})^{d(n)/d}$ and define the integer $g_{\mathfrak{r}}(n)$ by the largest power of p which satisfies $\beta_{\mathfrak{r},n}\in(M_{\infty,n,p}^\times)^{g_{\mathfrak{r}}(n)}$ ($M_{\infty,n,p}$ is the completion of $M_{\infty,n}$ for a prime divisor above p). Further let

$$g(n) = \min\{g_{\mathfrak{r}}(n)\mid \mathfrak{r}:\text{prime ideals of } F \text{ lying above a rational prime } r\equiv 1\,(\mathrm{mod}\, nN_F)\}.$$

Our main theorem is as follows.

Theorem 2. *Write*

$$X_{\omega\chi^{-1}}/(\gamma-\kappa(\gamma))X_{\omega\chi^{-1}} = \bigoplus_{i=1}^{t} \mathcal{O}_\chi/p^{e_i}, \quad e_1\geqslant\cdots\geqslant e_t$$

as $\mathcal{O}_\chi$-modules. Then we have

$$p^{e_{i+1}+\cdots+e_t} = \min\{g(n) \mid n \in \mathsf{S}_i\},$$

for any i, $0 \leqslant i \leqslant t-1$.

For any $\mathcal{O}_\chi$-module Y, we define the χ-rank of Y by $\dim_{\mathcal{O}_\chi/p}(Y \otimes_{\mathcal{O}_\chi} \mathcal{O}_\chi/p)$.

From the theorem, we get the following corollary immediately, because $\dim_{\mathcal{O}_\chi/p}(X_{\omega\chi^{-1}}/(\gamma-\kappa(\gamma))X_{\omega\chi^{-1}} \otimes_{\mathcal{O}_\chi} \mathcal{O}_\chi/p) = \dim_{\mathcal{O}_\chi/p}(X_{\omega\chi^{-1}}/(\gamma-1)X_{\omega\chi^{-1}} \otimes_{\mathcal{O}_\chi} \mathcal{O}_\chi/p)$.

Corollary 1. *The χ-rank of $A_{F,\omega\chi^{-1}}$ is smaller than or equal to i if and only if* $\min\{g(n) \mid n \in \mathsf{S}_i\} = 1$.

Corollary 2. *Let F'/F be the maximal abelian pro-p extension unramified outside p, and $\mathcal{T}$ the $\mathbb{Z}_p$-torsion subgroup of* $\mathrm{Gal}(F'/F)$. *Then $\mathcal{T}_\chi \simeq \oplus_{i=1}^{t} \mathcal{O}_\chi/p^{e_i}$ with e_i as in Theorem* 2.

Let $\mathcal{U}^{(1)} = \prod_{\mathfrak{p}|p} \mathcal{U}_\mathfrak{p}^{(1)}$, where $\mathfrak{p}$ runs over all prime ideal of F over p. By the natural injection $F^\times \hookrightarrow \prod_{\mathfrak{p}|p} F_\mathfrak{p}^\times$, we can regard $\beta_{\mathfrak{r},1}^{\nu-1}$ as an element of $\mathcal{U}^{(1)}$. Let $\mathcal{G}$ be the closure of the image of

$$\{\beta_{\mathfrak{r},1}^{\nu-1} \mid \mathfrak{r}\text{: prime ideal of } F \text{ lying above a rational prime } r \equiv 1 \pmod{N_F}\}$$

in $\mathcal{U}^{(1)}$. We get the following equation of the order of $X_{\omega\chi^{-1}}/(\gamma-\kappa(\gamma))X_{\omega\chi^{-1}}$ and that of $\mathcal{U}_\chi^{(1)}/\mathcal{G}_\chi$.

Corollary 3 (Ichimura and Hachimori [4, Theorem 1.2]).

$$|\mathcal{U}_\chi^{(1)}/\mathcal{G}_\chi| = |X_{\omega\chi^{-1}}/(\gamma-\kappa(\gamma))X_{\omega\chi^{-1}}|.$$

Ichimura and Hachimori also studied the order of $\mathcal{U}_\chi^{(1)}/\mathcal{G}_\chi$ for the characters $\chi(p) = 1$ or $\omega\chi^{-1}(p) = 1$.

In the case $F = \mathbb{Q}(\mu_p)$, Iwasawa [5] showed that $\mathcal{U}_\chi^{(1)} = \mathcal{G}_\chi$ for every odd character χ $(\neq\omega)$ of Δ implies $A_F^+ = 0$ (the conjecture of Vandiver).

We will give the proofs of Corollaries 2 and 3 in Section 4.4 together with that of Theorem 2.

2. Preliminary lemmas

2.1. For a field K, we denote the maximal abelian extension of K by K^{ab}. Let F, F_m and F_∞ be as in Section 1, and fix a prime ideal $\mathfrak{p}$ of F above p. We denote the

decomposition group and the inertia group of the prime ideal above $\mathfrak{p}$ in $\mathrm{Gal}(F_m^{\mathrm{ab}}/F_m)$ by D_m and I_m, respectively. Let $F_{m,\mathfrak{p}}$ be the completion at the prime ideal above $\mathfrak{p}$. We can regard D_m as the Galois group of $F_{m,\mathfrak{p}}^{\mathrm{ab}}/F_{m,\mathfrak{p}}$. We have an exact sequence

$$0 \to I_m \to D_m \to \mathrm{Gal}(\mathbb{F}_q^{\mathrm{ab}}/\mathbb{F}_q) \to 0,$$

where $\mathbb{F}_q$ is the residue field of $F_{m,\mathfrak{p}}$.

Let D be the decomposition group of p in $\Delta = \mathrm{Gal}(F/\mathbb{Q})$. The above sequence is exact as D-modules. For our fixed odd character χ, we denote the restriction of $\omega\chi^{-1}$ to D by $\omega\chi_D^{-1}$. Since we assumed $\omega\chi^{-1}(p) \neq 1$, we get $\omega\chi_D^{-1}$ is not the trivial character. Hence, we have the following isomorphism from the above exact sequence

$$(I_m \otimes_{\mathbb{Z}} \mathbb{Z}_p)_{\omega\chi_D^{-1}} \simeq (D_m \otimes_{\mathbb{Z}} \mathbb{Z}_p)_{\omega\chi_D^{-1}}. \tag{2.1.1}$$

Let $F_m^{\omega\chi_D^{-1}}$ be the subfield of F_m^{ab}/F_m such that

$$\mathrm{Gal}(F_m^{\omega\chi_D^{-1}}/F_m) \simeq (\mathrm{Gal}(F_m^{\mathrm{ab}}/F_m) \otimes_{\mathbb{Z}} \mathbb{Z}_p)_{\omega\chi_D^{-1}}.$$

Isomorphism (2.1.1) implies that the decomposition group of the prime ideal above $\mathfrak{p}$ in $\mathrm{Gal}(F_m^{\omega\chi_D^{-1}}/F_m)$ coincides with the inertia group.

We define $F_\infty^{\omega\chi_D^{-1}}$ in the same way. By taking the projective limit, we know that the decomposition group of the prime divisor above $\mathfrak{p}$ in $\mathrm{Gal}(F_\infty^{\omega\chi_D^{-1}}/F_\infty)$ coincides with the inertia group.

2.2. Let L_∞ denote the maximal unramified abelian pro-p extension over F_∞. In this section, we will consider the Kummer extension L_∞/F_∞. By the Kummer theory, there is a subgroup

$$V \subseteq F_\infty^\times \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p,$$

such that

$$L_\infty = F_\infty(\{a^{1/p^m} \mid a \otimes 1/p^m \in V\}),$$

and there exists a Kummer pairing

$$X \times V \to \mu_{p^\infty},$$

$$(x, a \otimes 1/p^m) \mapsto \langle x, a \otimes 1/p^m \rangle = (a^{1/p^m})^{x-1}, \tag{2.2.1}$$

where μ_{p^∞} denotes the group consisting of all p^mth root of unities for all $m \geqslant 0$. This is a non-degenerate bilinear pairing, and for any τ in $\mathrm{Gal}(F_\infty/\mathbb{Q})$, we have

$$\langle x, a \otimes 1/p^m \rangle^\tau = \langle x^\tau, a^\tau \otimes 1/p^m \rangle.$$

Recall

$$\Delta = \mathrm{Gal}(F/\mathbb{Q}), \quad \Gamma = \mathrm{Gal}(F_\infty/F).$$

By our assumption $p \nmid [F\colon \mathbb{Q}]$, we have

$$\mathrm{Gal}(F_\infty/\mathbb{Q}) \simeq \Delta \times \Gamma.$$

Let $(V^\Gamma)^\perp$ denote the annihilator of V^Γ in X with respect to the pairing (2.2.1), namely

$$(V^\Gamma)^\perp = \{x \in X \mid \langle x, v \rangle = 1, \text{ for every } v \in V^\Gamma\}.$$

Lemma 1. $(V^\Gamma)^\perp = (\gamma - \kappa(r))X$.

Proof. The proof is standard, so we will sketch it. First, let $(\gamma - \kappa(\gamma))x$ be an element of $(\gamma - \kappa(\gamma))X$. For every $v \in V^\Gamma$, we have $\langle (\gamma - \kappa(r))x, v \rangle = 1$. Hence we get $(V^\Gamma)^\perp \supset (\gamma - \kappa(\gamma))X$.

Next, let us prove the inclusion

$$(V^\Gamma)^\perp \subset (\gamma - \kappa(r))X. \tag{2.2.2}$$

Let

$$\{(\gamma - \kappa(\gamma))X\}^\perp = \{v \in V \mid \langle \sigma, v \rangle = 1, \text{ for every } x \in (\gamma - \kappa(\gamma))X\}$$

denote the annihilator of $(\gamma - \kappa(\gamma))X$ in V with respect to pairing (2.2.1). We will show the inclusion

$$V^\Gamma \supset \{(\gamma - \kappa(\gamma))X\}^\perp,$$

because this implies inclusion (2.2.2). Let v be an element of $\{(\gamma - \kappa(\gamma))X\}^\perp$. For every $x \in X$, we have $\langle x, v^{\gamma^{-1}-1} \rangle = 1$. Since pairing (2.2.1) is non-degenerate, we have $v^{\gamma^{-1}-1} = 1$. We conclude that v is an element of V^Γ. $\square$

By Lemma 1, we have the following non-degenerate bilinear pairing.

$$X/(\gamma - \kappa(\gamma))X \times V^\Gamma \to \mu_{p^\infty}. \tag{2.2.3}$$

Further, from the same arguments of [10, Section 10.2] we have the following non-degenerate bilinear pairing:

$$X_{\omega\chi^{-1}}/(\gamma-\kappa(\gamma))X_{\omega\chi^{-1}} \times V_\chi^\Gamma \to \mu_{p^\infty} \otimes_{\mathbb{Z}_p} \mathcal{O}_\chi. \tag{2.2.4}$$

2.3. Let $K/\mathbb{Q}$ be a Galois extension, not necessarily finite with Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$. Let I_K denote the ideal group of K, Cl_K the ideal class group of K, and A_K the Sylow p-subgroup of Cl_K.

For an infinite number field K, these groups are defined as follows.

$$I_K = \varinjlim I_{K_i}, \quad \mathrm{Cl}_K = \varinjlim \mathrm{Cl}_{K_i}, \quad A_K = \varinjlim A_{K_i},$$

where K_i runs over all subfields $\mathbb{Q} \subset K_i \subset K$ such that K_i is finite over $\mathbb{Q}$.

We define a $\mathbb{Z}_p[G]$-submodule W_K of $K^\times \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p$:

$$W_K = \{a \otimes 1/p^m \in K^\times \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \mid (a) \in p^m I_K\}.$$

We can easily show the following sequence:

$$0 \to E_K \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \to W_K \xrightarrow{\varphi} A_K \to 0 \tag{2.3.1}$$

is exact where E_K denotes the group of units in K, and the map φ is defined by

$$\varphi(a \otimes 1/p^m) = \text{class of } \mathfrak{a}, \quad \text{where } (a) = \mathfrak{a}^{p^m}, \ \mathfrak{a} \in I_K.$$

From now on, we assume that K is a CM-field. Let J denote the complex conjugation in $G = \mathrm{Gal}(K/\mathbb{Q})$. For any $\mathbb{Z}_p[G]$-module M, we define the submodule M^+ and M^- by

$$M^\pm = \{x \mid \in M, \ Jx = \pm x\}.$$

Since we assumed $p > 2$, we have $M = M^+ \oplus M^-$.

Lemma 2. $W_K^- \simeq A_K^-$.

Proof. Since $p > 2$, from the exact sequence (2.3.1), we have

$$0 \to (E_K \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p)^- \to W_L^- \to A_L^- \to 0.$$

Since $(E_K \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p)^- = 0$ (cf. [10, Theorem 4.12]), we obtain the assertion. □

2.4. Let K be an algebraic extension of $\mathbb{Q}$ (resp. $\mathbb{Q}_p$), not necessarily finite over $\mathbb{Q}$ (resp. $\mathbb{Q}_p$). We consider F satisfying the conditions in Section 1 with Galois group $\Delta = \mathrm{Gal}(F/\mathbb{Q})$, and an odd character $\chi(\neq\omega)$.

Lemma 3. *Assume that $K/\mathbb{Q}$ is an abelian extension with Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$ and there exists a subfield K' of K such that $K' \cap F = \mathbb{Q}$ and $K = FK'$. Then we can consider $\Delta = \mathrm{Gal}(F/\mathbb{Q})$ to be a subgroup of $G = \mathrm{Gal}(K/\mathbb{Q})$. For every intermediate field K_0 of F and K, we have isomorphisms of $\mathcal{O}_\chi$-modules*:

(1) $(K^\times/(K^\times)^{p^m})^H_\chi \simeq (K_0^\times/(K_0^\times)^{p^m})_\chi$, *for every* $m>0$,
(2) $(K^\times \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p)^H_\chi \simeq (K_0^\times \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p)_\chi$,

where $H = \mathrm{Gal}(K/K_0)$.

Proof. See [9, Lemma 2.2] for (1). By taking the direct limit of (1), we get (2). □

Lemma 4. (1) *If K satisfies the conditions of Lemma* 3, *then for every element $a \otimes 1/p^m \in (K^\times \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p)_\chi$, $a \otimes 1/p^m = 0$ if and only if $a = b^{p^m}$ for some $b \in K^\times$.*

(2) *If K contains μ_{p^∞}, then for every element $a \otimes 1/p^m \in K^\times \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p$, $a \otimes 1/p^m = 0$ if and only if $a = b^{p^m}$ for some $b \in K^\times$.*

Proof. It is obvious in both cases that $a = b^{p^m}$ implies $a \otimes 1/p^m = 0$. From the definition, $a \otimes 1/p^m = 0$ if and only if $a^{p^n} = b^{p^{n+m}}$ for some $b \in K^\times$ and some $n \geqslant 0$. In case (1), this implies $a = b^{p^m}$ because the map $(K^\times \otimes_{\mathbb{Z}} 1/p^n\mathbb{Z}/\mathbb{Z})_\chi \to (K^\times \otimes_{\mathbb{Z}} 1/p^{n+1}\mathbb{Z}/\mathbb{Z})_\chi$ is injective for any $n>0$. In case (2), $a^{p^n} = b^{p^{n+m}}$ implies $a = b^{p^m}\zeta$ for some $\zeta \in \mu_{p^n}$ and we have $a = b^{p^m}\zeta \in (K^\times)^{p^m}$ because K contains μ_{p^∞}. □

We get the following lemma as an immediate corollary of Lemma 4.

Lemma 5. (1) *Assume that K satisfies the conditions of Lemma* 3. *Let $a \otimes 1/p^m$ be an element of $(K^\times \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p)_\chi$ such that $a \notin (K^\times)^p$. Then we have $\langle a \otimes 1/p^m \rangle_{\mathcal{O}_\chi} \simeq \mathcal{O}_\chi/p^m$ as $\mathcal{O}_\chi$-modules. Hence, we see $|\langle a \otimes 1/p^m \rangle_{\mathcal{O}_\chi}| = q^m$ with $q = |\mathcal{O}_\chi/p|$.*

(2) *Assume that K contains μ_{p^∞}. Let $a \otimes 1/p^m$ be an element of $K^\times \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p$ such that $a \notin (K^\times)^p$. Then we have $\langle a \otimes 1/p^m \rangle_{\mathbb{Z}} \simeq \mathbb{Z}/p^m$ as abelian groups.*

3. Gauss sums

3.1. We will review the definition of Stickelberger elements and Gauss sums. We will also prove a small lemma which states the $\mathbb{Z}_p[\Delta]$-module W_F in Section 2.3 can be written as a set of Gauss sums.

Let $N>0$ be an integer. We identify $\mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q})$ with $(\mathbb{Z}/N)^\times$ in the usual way, and denote the isomorphism by

$$\mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q}) \simeq (\mathbb{Z}/N)^\times,$$

$$\sigma_a \leftrightarrow a \bmod N.$$

Define the Stickelberger element θ_N by

$$\theta_N = \sum_{\substack{a=1 \\ (a,N)=1}}^{N} \frac{a}{N}\sigma_a^{-1} \in \mathbb{Q}[\mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q})].$$

Let F be as in Section 1 with Galois group $\Delta = \mathrm{Gal}(F/\mathbb{Q})$. Let N_F denotes the conductor of F. By the definition of F, N_F is the least common multiple of the conductor of χ and p.

For each prime ideal $\mathfrak{R}$ of $\mathbb{Q}(\mu_{N_F})$ which splits completely in $\mathbb{Q}(\mu_{N_F})/\mathbb{Q}$, we define the character $\chi_{\mathfrak{R}} : (\mathbb{Z}/r)^\times \to \mu_{N_F}$ (r is the rational prime below $\mathfrak{R}$) which is given by

$$\chi_{\mathfrak{R}}(a) \equiv a^{-(r-1)/N_F} \bmod \mathfrak{R}.$$

We define the Gauss sum $\tau_{\mathfrak{R}}$ by

$$\tau_{\mathfrak{R}} = \sum_{a=1}^{r-1} \chi_{\mathfrak{R}}(a)\zeta_r^a \in \mathbb{Q}(\mu_{rN_F})^\times,$$

where ζ_r is a fixed primitive rth root of unity.

For the prime ideal $\mathfrak{r}$ of F below $\mathfrak{R}$, we define

$$\tau_{\mathfrak{r}} = \mathrm{Norm}(\tau_{\mathfrak{R}}) \in F(\mu_r)^\times,$$

where $\mathrm{Norm} : \mathbb{Q}(\mu_{rN_F})^\times \to F(\mu_r)^\times$ is the norm map. $\tau_{\mathfrak{r}}$ is well defined because of $\tau_{\mathfrak{R}^\sigma} = \tau_{\mathfrak{R}}^\sigma$ for any $\sigma \in \mathrm{Gal}(\mathbb{Q}(\mu_{rN_F})/F(\mu_r))$.

We consider the fixed odd character $\chi(\neq\omega)$ of Δ as a character of $\mathrm{Gal}(\mathbb{Q}(\mu_{rN_F})/\mathbb{Q})$. We choose $\sigma_\alpha \in \mathrm{Gal}(\mathbb{Q}(\mu_{N_F})/\mathbb{Q})$ such that $\chi(\sigma_\alpha) - \alpha$ is invertible in $\mathcal{O}_\chi$.

By Stickelberger's theorem, we have

$$(\tau_{\mathfrak{r}}^{(\chi(\sigma_\alpha)-\alpha)e_\chi}) = (\chi(\sigma_\alpha) - \alpha)\theta_{N_F,\chi}\mathfrak{r}_\chi$$

in $(I_F \otimes_{\mathbb{Z}} \mathbb{Z}_p)_\chi$. Since $\chi(\sigma_\alpha) - \alpha \in \mathcal{O}_\chi^\times$, we have

$$(\tau_{\mathfrak{r}}^{e_\chi}) = \theta_{N_F,\chi}\mathfrak{r}_\chi, \tag{3.1.1}$$

in $(I_F \otimes_{\mathbb{Z}} \mathbb{Z}_p)_\chi$. We see

$$\theta_{N_F,\chi} = (1 - \chi^{-1}(p))B_{1,\chi^{-1}},$$

where $B_{1,\chi^{-1}}$ denotes the generalized Bernoulli number. By the assumption $\chi(p)\neq 1$, we have $\theta_{N_F,\chi}\sim B_{1,\chi^{-1}}$, here, $\sim$ means that both sides have the same p-adic valuation. Let $f=[\mathcal{O}_\chi\colon \mathbb{Z}_p]$ and the integer $d>0$ such that $d^f=|A_{F,\chi}|$. By the theorem of Mazur and Wiles [7], we have $B_{1,\chi^{-1}}\sim d$. Hence we can write $\theta_{N_F,\chi}=ud$, for some $u\in\mathcal{O}_\chi^\times$. Define the element η of $\mathbb{Z}_p[\Delta]$ by

$$\mathcal{O}_\chi\simeq\mathcal{O}_\chi e_\chi\simeq\mathbb{Z}_p[\Delta]e_\chi,$$

$$u^{-1}\mapsto u^{-1}e_\chi\mapsto\eta e_\chi.$$

From (3.1.1), we have

$$(\tau_{\mathfrak{r}}^{\eta e_\chi})=d\mathfrak{r}_\chi \tag{3.1.2}$$

in $(I_F\otimes_{\mathbb{Z}}\mathbb{Z}_p)_\chi$.

Let $\bar{e}_\chi$ and $\bar{\eta}$ be elements of $\mathbb{Z}[\Delta]$ such that $\bar{e}_\chi\equiv e_\chi\pmod d$ and $\bar{\eta}\equiv\eta\pmod d$.

Fix an integer $k>0$, and define a subset $W(1)$ of $(F^\times\otimes_{\mathbb{Z}}\mathbb{Q}_p/\mathbb{Z}_p)_\chi$ by

$W(1)=\{\tau_{\mathfrak{r}}^{\bar{e}_\chi}\otimes 1/d=(\tau_{\mathfrak{r}}\otimes 1/d)e_\chi\mid \mathfrak{r}\colon$ prime ideals of F lying above a rational prime $r\equiv 1\pmod{kN_F}\}$.

Lemma 6. *Let W_F be as in Section 2.3. For any integer $k>0$, we have $W_{F,\chi}=W(1)$. Especially, the set $W(1)$ is an $\mathcal{O}_\chi$-module and it is independent of an integer k.*

Proof. Put

$W'(1)=\{\tau_{\mathfrak{r}}^{\bar{e}_\chi\bar{\eta}}\otimes 1/d=(\tau_{\mathfrak{r}}\otimes 1/d)e_\chi\eta\mid \mathfrak{r}\colon$ prime ideals of F lying above a rational prime $r\equiv 1\pmod{kN_F}\}$.

If we show an equality $W_{F,\chi}=W'(1)$, then $W'(1)$ is an $\mathcal{O}_\chi$-module, so we have $W_{F,\chi}=W'(1)=uW'(1)=W(1)$. Hence we will show the equality $W_{F,\chi}=W'(1)$. By (3.1.2), it is sufficient to show the inclusion $W_{F,\chi}\subset W'(1)$. Recall

$$W_{F,\chi}=\{a\otimes 1/p^m\in(F^\times\otimes_{\mathbb{Z}}\mathbb{Q}_p/\mathbb{Z}_p)_\chi\mid(a)\in p^mI_F\}.$$

Let $a\otimes 1/p^m$ be an element of $W_{F,\chi}$. Suppose $p^m>d$. From the isomorphism of $\mathcal{O}_\chi$-modules $W_{F,\chi}\simeq A_{F,\chi}$ (Lemma 2), we see $a\otimes d/p^m=0$. By Lemma 4(1), we can write $a=b^{p^m/d}$, for some $b\in F^\times$. Hence we have

$$a\otimes 1/p^m=b^{p^m/d}\otimes 1/p^m=b\otimes 1/d.$$

Thus we may assume $p^m\leqslant d$.

Since $a\otimes 1/p^m$ is an element of $W_{F,\chi}$, we can write $(a)=p^m\mathfrak{a}$, for some $\mathfrak{a}\in I_F$. Let $c\in A_{F,\chi}$ be the ideal class of $\mathfrak{a}$. By the Chebotarev density theorem, we can choose a prime ideal $\mathfrak{r}$ of F lying above a rational prime $r\equiv 1\pmod{kN_F}$, and whose class

is c. Write $\mathfrak{r} = \mathfrak{a}(b)$, for some $b \in F^\times$. Then

$$(a^{d/p^m} b^d)^{e_\chi} = d\mathfrak{a}_\chi + (b^{e_\chi d})$$
$$= d\mathfrak{r}_\chi,$$

in $(I_F \otimes_{\mathbb{Z}} \mathbb{Z}_p)_\chi$. From this and (3.1.2), we have $(\tau_{\mathfrak{r}}^{\eta e_\chi}) = (a^{d/p^m} b^d)^{e_\chi}$ in $(I_F \otimes_{\mathbb{Z}} \mathbb{Z}_p)_\chi$. Since $(E_F \otimes_{\mathbb{Z}} \mathbb{Z}_p)_\chi = 0$, we have $\tau_{\mathfrak{r}}^{\eta e_\chi} = (a^{d/p^m} b^d)^{e_\chi}$ in $(F^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p)_\chi$. Hence

$$a \otimes 1/p^m = a^{d/p^m} b^d \otimes 1/d = (\tau_{\mathfrak{r}} \otimes 1/d) e_\chi \eta$$

in $(F^\times \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p)_\chi$. □

3.2. In this section, we will review a result of Rubin [9] which is obtained from arguments of the Euler system of Gauss sums.

Let M be a power of p such that $M > |A(F)_\chi|^2$. For any integer $i \geqslant 0$, let S_i denote the set of positive squarefree integers which are divisible by exactly i primes ℓ which satisfy $\ell \equiv 1 \pmod{MN_F}$. Let $\mathsf{S} = \bigcup_{i \geqslant 0} \mathsf{S}_i$. For each prime $\ell \in \mathsf{S}$, fix a generator σ_ℓ of $\mathrm{Gal}(F(\mu_\ell)/F) \simeq \mathrm{Gal}(\mathbb{Q}(\mu_\ell/\mathbb{Q})$, and let

$$D_\ell = \sum_{i=0}^{\ell-2} i\sigma_\ell^i.$$

For each $n \in \mathsf{S}$, let

$$D_n = \prod_{\ell | n} D_\ell, \quad N_n = \sum_{\tau \in G_n} \tau,$$

where $G_n = \mathrm{Gal}(F(\mu_n)/F) \simeq \mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})$.

We define $\delta(n) \in (\mathbb{Z}/M)[\Delta]$ to be the element satisfying $D_n(\sigma_\alpha - \alpha)\theta_{nN_F} = N_n \delta(n)$ (see [1,9] for the precise and see [2] for the explicit formula for $\delta(n)$).

Let $d(n)$ be the largest power of p which divides $\delta(n)_\chi \in (\mathcal{O}_\chi/M)e_\chi$. Note that $d(1) = d \sim B_{1,\chi^{-1}}$.

For each $n \in \mathsf{S}$, let $T(n)$ denote the $\mathcal{O}_\chi$-submodule of $(F^\times \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p)_\chi$. which is generated by the elements $(\tau_{\mathfrak{r}} \otimes 1/d)e_\chi$ where $\mathfrak{r}$ divides n. By Lemma 6, $T(n)$ is also an $\mathcal{O}_\chi$-submodule of $W_{F,\chi}$. If $n \in \mathsf{S}_i$, then $T(n)$ is generated by i elements, because

$$(\tau_{\mathfrak{r}^\sigma} \otimes 1/d)e_\chi = (\tau_{\mathfrak{r}}^\sigma \otimes 1/d)e_\chi = (\tau_{\mathfrak{r}} \otimes 1/d)\chi(\sigma)e_\chi,$$

for any $\sigma \in \Delta$. By the definition, for n, $m \in \mathsf{S}$ such that n divides m, we have $0 = T(1) \subset T(n) \subset T(m)$.

For each $n \in \mathsf{S}$, let $B_F(n)$ denote the $\mathbb{Z}_p[\Delta]$- submodule of A_F which is generated by the classes of prime ideals of F dividing n. By the isomorphism of Lemma 2 and

(3.1.2), we have

$$\begin{array}{ccc} W_{F,\chi} & \simeq & A_{F,\chi} \\ \cup & & \cup \\ T(n) & \simeq & B_F(n)_\chi \\ \cup & & \cup \\ \langle (\tau_{\mathfrak{r}} \otimes 1/d)e_\chi \rangle_{\mathcal{O}_\chi} & \simeq & \langle [\mathfrak{r}_\chi] \rangle_{\mathcal{O}_\chi}. \end{array} \tag{3.2.3}$$

Hence

$$W_{F,\chi}/T(n) \simeq A_{F,\chi}/B_F(n)_\chi. \tag{3.2.4}$$

Rubin [9] showed the following inequality for $F = \mathbb{Q}(\mu_p)$ by using arguments of the Euler system of Gauss sums. As he mentioned the remark at the end of [9], the result is equally shown for our F, because we assume $p \nmid [F : \mathbb{Q}]$.

Proposition 1 (Rubin [9, Corollary 4.2]). *For each $n \in \mathsf{S}$, we have*

$$|A_{F,\chi}/B_F(n)_\chi| \leqslant d(n)^f,$$

where $f = [\mathcal{O}_\chi : \mathbb{Z}_p]$.

Hence from (3.2.4), we have

$$|W_{F,\chi}/T(n)| \leqslant d(n)^f, \tag{3.2.5}$$

for each $n \in \mathsf{S}$.

4. Proofs

4.1. In Section 4, we will give the proofs of our main results in Section 1. Recall that our aim is to determine the structure of $\mathcal{O}_\chi$-module $X_{\omega\chi^{-1}}/(\gamma - \kappa(\gamma))X_{\omega\chi^{-1}}$ in Section 2.2. We will begin with the following lemma.

Lemma 7. *Let V^Γ be as in Section* 2.2, *and W_F be as in Section* 2.3. *Then V^Γ_χ is an $\mathcal{O}_\chi$-submodule of $W_{F,\chi}$.*

Proof. By the definition, we have $V^\Gamma_\chi \subset (F^\times_\infty \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p)^\Gamma_\chi$. By Lemma 3, we have an isomorphism of $\mathcal{O}_\chi$-modules $(F^\times_\infty \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p)^\Gamma_\chi \simeq (F^\times \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p)_\chi$. Hence we can regard V^Γ_χ as an $\mathcal{O}_\chi$-submodule of $(F^\times \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p)_\chi$.

Let $a\otimes 1/p^m (a\in F^\times)$ be an element of V_χ^Γ. Since $a\otimes 1/p^m$ gives an unramified extension, it follows that

$$(a)=\mathfrak{b}^{p^m} \quad \text{in } I_{F_n},$$

for some $n\geqslant m$, and $\mathfrak{b}\in I_{F_n}$. Since F_n/F is unramified outside p, we have

$$(a)=\mathfrak{a}^{p^m}\mathfrak{a}' \quad \text{in } I_F,$$

where $\mathfrak{a},\mathfrak{a}'\in I_F$ and $\mathfrak{a}'$ is a product of primes above p. It is sufficient to show

$$(a)=(a^{e_\chi})=e_\chi\mathfrak{a}'=0 \quad \text{in } I_F/p^m I_F.$$

Let $I_{F,p}$ be subgroup of I_F which is generated by primes above p. Since our assumption $\chi(p)\neq 1$, we get

$$(I_{F,p}\otimes_{\mathbb{Z}}\mathbb{Z}_p)_\chi\simeq\mathbb{Z}_p[\Delta/D]_\chi=0,$$

where D is the decomposition group of p. The above assertion follows from this. □

By Lemma 7, V_χ^Γ is finite because $W_{F,\chi}\simeq A_{F,\chi}$ is a finite group. Hence from pairing (2.2.4), we have a noncanonical isomorphism of $\mathcal{O}_\chi$-modules:

$$X_{\omega\chi^{-1}}/(\gamma-\kappa(\gamma))X_{\omega\chi^{-1}}\simeq V_\chi^\Gamma \tag{4.1.1}$$

(cf. [10, Lemmma 3.1]). We will study the structure of V_χ^Γ instead of $X_{\omega\chi^{-1}}/(\gamma-\kappa(\gamma))X_{\omega\chi^{-1}}$.

By Lemma 3, we can regard $W_{F,\chi}$, V_χ^Γ, $T(n)$ $(n\in\mathbf{S})$ as $\mathcal{O}_\chi$-submodules of $(F_\infty^\times\otimes_{\mathbb{Z}}\mathbb{Q}_p/\mathbb{Z}_p)_\chi^\Gamma$.

Let

$$M_\infty=F_\infty(\{a^{1/p^m}\mid a\otimes 1/p^m\in W_{F,\chi}\}),$$

$$L_{\infty,0}=F_\infty(\{a^{1/p^m}\mid a\otimes 1/p^m\in V_\chi^\Gamma\}),$$

and for any $n\in\mathbf{S}$, let

$$M_{\infty,n}=F_\infty(\{a^{1/p^m}\mid a\otimes 1/p^m\in T(n)\}).$$

M_∞/F_∞ is a finite abelian p-extension unramified outside p. Every intermediate field K of F_∞ and M_∞ which corresponds to an $\mathcal{O}_\chi$-submodule Y of $W_{F,\chi}$ is a Galois extension over $\mathbb{Q}$, because Δ acts on Y via χ and Γ acts on Y trivially.

Recall that L_∞ is the maximal unramified abelian p-extension over F_∞. Since $V\cap W_{F,\chi}=V_\chi^\Gamma$, we have $L_\infty\cap M_\infty=L_{\infty,0}$. Hence $L_{\infty,0}$ (resp. $M_{\infty,n}L_{\infty,0}$) is the

maximal unramified extension of F_∞ (resp. $M_{\infty,n}$) contained in M_∞.

$$\begin{array}{ccccc} M_{\infty,n} & \overset{\text{u.r.}}{-} & M_{\infty,n}L_{\infty,0} & - & M_\infty \\ | & & | & & \\ F_\infty \overset{\text{u.r.}}{-} M_{\infty,n}\cap L_{\infty,0} & \overset{\text{u.r.}}{-} & L_{\infty,0} & & \end{array} \tag{4.1.2}$$

Here, u.r. means an unramified extension. The rest of Section 4.1 is devoted to the study of the Kummer extension $M_\infty/M_{\infty,n}$ with $n\in\mathsf{S}$.

Lemma 8. *For any $n\in\mathsf{S}$, $M_{\infty,n}$ is a CM-field.*

Proof. Since $M_{\infty,n}/F_\infty$ is a Galois extension and F_∞ is a totally imaginary field, $M_{\infty,n}$ is also totally imaginary field. Let J denote the complex conjugation and $\langle J\rangle$ the Galois group which is generated by J. We have

$$\begin{array}{ccccc} F_\infty & - & M_{\infty,n} & & \\ \langle J\rangle \quad | & & | & \quad \langle J\rangle & \\ {F_\infty}^+ & - & {M_{\infty,n}}^{\langle J\rangle} & & \\ | & & & & \\ \mathbb{Q} & & & & \end{array}$$

where F_∞^+ is the maximal real subfield of F_∞, and $M_{\infty,n}^{\langle J\rangle}$ is the fixed field of J contained in $M_{\infty,n}$.

Since J acts on $\mathrm{Gal}(M_{\infty,n}/F_\infty)$ via $\omega\chi^{-1}$ and χ is an odd character, we have $\sigma^J = J\sigma J^{-1} = \sigma$, for every $\sigma\in\mathrm{Gal}(M_{\infty,n}/F_\infty)$. Hence J and every element of $\mathrm{Gal}(M_{\infty,n}/F_\infty)$ are commutative. It follows from this that $M_{\infty,n}^{\langle J\rangle}/F_\infty^+$ is a Galois extension. Since F_∞^+ is a totally real field and 2 does not divide $[M_{\infty,n}^{\langle J\rangle} : F_\infty^+]$, $M_{\infty,n}^{\langle J\rangle}$ is a totally real field. □

For each $n\in\mathsf{S}$, let

$$\psi_n\colon F_\infty^\times\otimes_{\mathbb{Z}}\mathbb{Q}_p/\mathbb{Z}_p \to M_{\infty,n}^\times\otimes_{\mathbb{Z}}\mathbb{Q}_p/\mathbb{Z}_p$$

be the natural map. Define

$$W(n) = \psi_n(W_{F,\chi}) \subset W^-_{M_{\infty,n}}$$

(cf. Section 2.3 for the definition of $W^-_{M_{\infty,n}}$). We have the following diagram of two

Kummer pairings:

$$\begin{array}{ccccc} \mathrm{Gal}(M_\infty/F_\infty) & \times & W_{F,\chi} & \to \mu_{p^\infty} \otimes_{\mathbb{Z}_p} \mathcal{O}_\chi \\ \uparrow & & \downarrow & \| \\ \mathrm{Gal}(M_\infty/M_{\infty,n}) & \times & W(n) & \to \mu_{p^\infty} \otimes_{\mathbb{Z}_p} \mathcal{O}_\chi \end{array}$$

and by the definition of $M_{\infty,n}$ and (4.1.2), we have an isomorphism of $\mathcal{O}_\chi$-modules:

$$W(n) \simeq W_{F,\chi}/T(n).$$

We know from (3.2.5),

$$[M_\infty : M_{\infty,n}] = |W(n)| \leqslant d(n)^f,$$

with $f = [\mathcal{O}_\chi : \mathbb{Z}_p]$.

Next, we will define an element $\beta_{\mathfrak{r},n}$ of $M_{\infty,n}^\times$ for each $n \in \mathsf{S}$ and each prime ideal of $\mathfrak{r}$ of F lying above a rational prime $r \equiv 1 \pmod{nN_F}$.

Lemma 9. *Let $n \in \mathsf{S}$ and $\mathfrak{r}$ be a prime ideal of F lying above a rational prime $r \equiv 1 \pmod{nN_F}$. Then $(\tau_\mathfrak{r}^{\bar{e}_\chi})^{d(n)/d}$ is an element of $M_{\infty,n}^\times$.*

Proof. We may assume $d(n) < d$. By the argument of Euler system of Gauss sums (cf. [1, Proposition 3.1; 9, Proposition 2.3]), we have

$$d(n)\mathfrak{r}_\chi = \mathfrak{a} + (a) \quad \text{in } (I_F \otimes_{\mathbb{Z}} \mathbb{Z}_p)_\chi,$$

where $\mathfrak{a}$ is a product of prime ideals dividing n and $a \in (F^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p)_\chi$. For the element $u \in \mathcal{O}_\chi^\times$ defined in Section 3.1, we have

$$d(n)\mathfrak{r}_\chi^u = (\mathfrak{a} + (a))^u.$$

By the definition of $M_{\infty,n}$, $\mathfrak{a}$ is principal in $M_{\infty,n}$. Hence we see

$$d(n)\mathfrak{r}_\chi^u = (b) \quad \text{in } I_{M_{\infty,n}} \otimes_{\mathbb{Z}} \mathbb{Z}_p,$$

for some $b \in M_{\infty,n}^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p$. For the complex conjugation J, we have

$$d(n)\mathfrak{r}_\chi^u = (b^{(1-J)/2}) \quad \text{in } I_{M_{\infty,n}} \otimes_{\mathbb{Z}} \mathbb{Z}_p.$$

Hence $\bar{b}^{1-J} \otimes 1/(2d(n))$ is an element of $W_{M_{\infty,n}}^-$, here $\bar{b}$ is an element of $M_{\infty,n}^\times$ such that $b \equiv \bar{b} \pmod{(M_{\infty,n}^\times)^{d(n)}}$. On the other hand, by Lemma 6, $\tau_\mathfrak{r}^{\bar{e}_\chi} \otimes 1/d$ is an element

of $W_{F,\chi}$. Considering the commutative diagram

$$\begin{array}{ccc} & W_{F,\chi} & \simeq & A_{F,\chi} \\ \psi_n & \downarrow & & \downarrow \\ & W_{M_{\infty,n}}{}^{-} & \simeq & A_{M_{\infty,n}}{}^{-}. \end{array}$$

From (3.1.2), the image of $\bar{b}^{1-J}\otimes 1/(2d(n))$ and that of $\tau_{\mathfrak{r}}^{\bar{e}_\chi}\otimes 1/d$ in $A^-_{M_{\infty,n}}$ are both $[\mathfrak{r}_\chi^u]$. Hence it follows from the isomorphism $W^-_{M_{\infty,n}}\simeq A^-_{M_{\infty,n}}$ that

$$\tau_{\mathfrak{r}}^{\bar{e}_\chi}\otimes 1/d=\bar{b}^{(1-J)ud/d(n)}\otimes 1/d \quad \text{in } M^\times_{\infty,n}\otimes_{\mathbb{Z}}\mathbb{Q}_p/\mathbb{Z}_p,$$

for some integer $u>0$. By Lemma 4(2), we get $\tau_{\mathfrak{r}}^{\bar{e}_\chi}\in(M^\times_{\infty,n})^{d/d(n)}$. This completes the proof. □

For each $n\in\mathsf{S}$ and each prime ideal $\mathfrak{r}$ of F lying above a rational prime $r\equiv 1\pmod{nN_F}$, define by the previous lemma,

$$\beta_{\mathfrak{r},n}=(\tau_{\mathfrak{r}}^{\bar{e}_\chi})^{d(n)/d}\in M^\times_{\infty,n}.$$

Remark. If $d(n)<d$, then $\beta_{\mathfrak{r},n}$ is not uniquely determined. Namely, there is a difference of $d/d(n)$th root of unity by the definition. But $(E_{M_{\infty,n}}\otimes_{\mathbb{Z}}\mathbb{Q}_p/\mathbb{Z}_p)^-=0$ implies that $\beta_{\mathfrak{r},n}\otimes 1/d(n)\in W^-_{M_{\infty,n}}$ is uniquely determined.

Recall the Kummer pairing

$$\mathrm{Gal}(M_\infty/M_{\infty,n})\times W(n)\to\mu_{p^\infty}\otimes_{\mathbb{Z}_p}\mathcal{O}_\chi$$

and

$$W(n)=\psi_n(W_{F,\chi})\subset W^-_{M_{\infty,n}},$$

for $n\in\mathsf{S}$.

The next lemma follows from Lemma 6 and the definition of $\beta_{\mathfrak{r},n}$.

Lemma 10. *For any $n\in\mathsf{S}$, we have*

$W(n)=\{\beta_{\mathfrak{r},n}\otimes 1/d(n)\mid \mathfrak{r}:$ *prime ideal of F lying above a rational prime $r\equiv 1\pmod{nN_F}$*$\}$.

4.2. In this subsection, we will prove the key proposition (Proposition 2) for the proof of Theorem 2. We will study the $\mathcal{O}_\chi$-module $V_\chi^\Gamma\simeq X_{\omega\chi^{-1}}/(\gamma-\kappa(\gamma))X_{\omega\chi^{-1}}$. Write

$$V_\chi^\Gamma=\bigoplus_{i=1}^{t}\mathcal{O}_\chi/p^{e_i},\quad e_1\geqslant\cdots\geqslant e_t, \tag{4.2.1}$$

$$\mathcal{O}_\chi/p^{e_i}\simeq\langle a_i\otimes 1/p^{m_i}\rangle_{\mathcal{O}_\chi}\quad (a_i\otimes 1/p^{m_i}\in(F^\times\otimes_{\mathbb{Z}}\mathbb{Q}_p/\mathbb{Z}_p)_\chi).$$

By Lemmas 6, 7 and the definition of $T(n)$ in Section 3.2, there exists $n \in \mathsf{S}_i$ such that $T(n) = \oplus_{j=1}^{i} \langle a_j \otimes 1/p^{m_j} \rangle_{\mathcal{O}_\chi}$, (note that $T(1) = 0$). Our aim in this subsection is the following proposition.

Proposition 2. *For any i, $0 \leqslant i \leqslant t$, there exists $n_i \in \mathsf{S}_i$ such that*

$$T(n_i) = \bigoplus_{j=1}^{i} \langle a_j \otimes 1/p^{m_j} \rangle_{\mathcal{O}_\chi}$$

and

$$|W(n_i)| = |W_{F,\chi}/T(n_i)| = d(n_i)^f.$$

Proof. We will choose $n_i \in \mathsf{S}_i$ inductively. There is nothing to do for $i = 0$. Suppose that there exists $n_i \in \mathsf{S}_i$ which satisfies the above conditions. By Lemma 6, we can write

$$a_{i+1} \otimes 1/p^{m_{i+1}} = (\tau_\rho \otimes 1/d) e_\chi,$$

for some prime ideal ρ of F lying above a rational prime $\ell \equiv 1 \pmod{n_i N_F M}$. By the same arguments in [9, the proof of Theorem 4.1], there exists a prime ideal $\mathfrak{r}$ of F lying above a rational prime $r \equiv 1 \pmod{n_i N_F M}$ with $d(n_i) \geqslant d(n_i r)$ such that

$$\langle [\mathfrak{r}_\chi] \rangle_{\mathcal{O}_\chi} = \langle [\rho_\chi] \rangle_{\mathcal{O}_\chi} \subset A_{F,\chi} \tag{4.2.2}$$

and

$$d(n_i)/d(n_i r)\rho_\chi = \mathfrak{a} + (a) \quad \text{in } (I_F \otimes_{\mathbb{Z}} \mathbb{Z}_p)_\chi,$$

where $\mathfrak{a}$ is a product of prime ideals dividing n_i and a is an element of $(F^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p)_\chi$.

Let $B_F(n_i)$ be the $\mathbb{Z}_p[\Delta]$-submodule of A_F which is defined in Section 3.2. From (3.2.3), we have

$$\begin{array}{ccc} W_{F,\chi} & \simeq & A_{F,\chi} \\ \cup & & \cup \\ T(n_i) \oplus \langle (\tau_\rho \otimes 1/d) e_\chi \rangle_{\mathcal{O}_\chi} & \simeq & B_F(n_i)_\chi \oplus \langle [\rho_\chi] \rangle_{\mathcal{O}_\chi}. \end{array}$$

From this and (4.2.2), we have

$$d(n_i)/d(n_i r)\rho_\chi = (b) \quad \text{in } (I_F \otimes_{\mathbb{Z}} \mathbb{Z}_p)_\chi,$$

for some $b \in (F^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p)_\chi$. For the element $u \in \mathcal{O}_\chi^\times$ defined in Section 3.1, we have

$$d(n_i)/d(n_i r)\rho_\chi^u = (b^u) \quad \text{in } (I_F \otimes_{\mathbb{Z}} \mathbb{Z}_p)_\chi.$$

Hence we get $b^u \otimes d(n_i r)/d(n_i) \in W_{F,\chi}$. The image of $b^u \otimes d(n_i r)/d(n_i)$ and that of $(\tau_\rho \otimes 1/d)e_\chi$ in $A_{F,\chi}$ are both $[\rho_\chi^u]$, so it follows that

$$\begin{aligned}\tau_\rho^{\bar{e}_\chi} \otimes 1/d &= (\tau_\rho \otimes 1/d)e_\chi \\ &= b^u \otimes d(n_i r)/d(n_i) \\ &= b^{u(dd(n_i r))/d(n_i)} \otimes 1/d.\end{aligned}$$

By Lemma 4(1), we have $\tau_\rho^{\bar{e}_\chi} \in (F^\times)^{(dd(n_i r))/d(n_i)}$.

Let $k \geqslant 0$ be the largest integer such that $\tau_\rho^{\bar{e}_\chi} \in (F^\times)^{p^k}$. Then we have $p^k \geqslant (dd(n_i r))/d(n_i)$. It follows from Lemma 5(1) that

$$|\langle \tau_\rho^{\bar{e}_\chi} \otimes 1/d \rangle_{\mathcal{O}_\chi}| = (d/p^k)^f \leqslant (d(n_i)/d(n_i r))^f, \tag{4.2.3}$$

where $f = [\mathcal{O}_\chi : \mathbb{Z}_p]$.

Let $n_{i+1} = n_i r \in \mathsf{S}_{i+1}$. From (4.2.2) and (4.2.3) we have

$$\begin{aligned}T(n_i) \oplus \langle a_{i+1} \otimes 1/p^{m_{i+1}} \rangle_{\mathcal{O}_\chi} &= T(n_i) \oplus \langle (\tau_{\mathfrak{r}} \otimes 1/d)e_\chi \rangle_{\mathcal{O}_\chi} \\ &= T(n_{i+1})\end{aligned}$$

and

$$\begin{aligned}|W(n_{i+1})| &= |W_{F,\chi}/T(n_{i+1})| \\ &= |W(n_i)|/|\langle (\tau_{\mathfrak{r}} \otimes 1/d)e_\chi \rangle_{\mathcal{O}_\chi}| \\ &\geqslant d(n_i)^f \times (d(n_{i+1})/d(n_i))^f \\ &= d(n_{i+1})^f.\end{aligned}$$

Using (3.2.5), we get the conclusion. □

4.3. Let M_∞ and $L_{\infty,0}$ be as in Section 4.1. Recall that $L_{\infty,0}$ is the maximal unramified extension of F_∞ contained in M_∞ (see (4.1.2)). In addition, from Section 2.1 we know that $L_{\infty,0}$ is the maximal extension of F_∞ contained in M_∞ in which every prime divisor of F_∞ lying above p is completely decomposed. Since M_∞/F_∞ is an extension unramified outside p, the group $\mathrm{Gal}(M_\infty/L_{\infty,0})$ is generated by decomposition groups in $\mathrm{Gal}(M_\infty/F_\infty)$ of prime divisors above p.

Fix a prime ideal $\mathfrak{p}$ of F lying above p, and let $M_{\infty,\mathfrak{p}}/F_{\infty,\mathfrak{p}}$ denote the completion of the extension at a prime divisor lying above $\mathfrak{p}$. Let D denote the decomposition group of p in $\Delta = \mathrm{Gal}(F/\mathbb{Q})$, and for any character ψ of Δ, let ψ_D denote the restriction of ψ to D. $\mathrm{Gal}(M_{\infty,\mathfrak{p}}/F_{\infty,\mathfrak{p}})$ is an $\mathcal{O}_{\chi_D}$-module because D acts on it via $\omega\chi_D^{-1}$. From the above arguments, we have $\mathrm{Gal}(M_\infty/L_{\infty,0}) = \langle \mathrm{Gal}(M_{\infty,\mathfrak{p}}/F_{\infty,\mathfrak{p}}) \rangle_{\mathcal{O}_\chi}$.

Lemma 11. $\mathrm{Gal}(M_{\infty,\mathfrak{p}}/F_{\infty,\mathfrak{p}})$ *is a finite cyclic* $\mathcal{O}_{\chi_D}$*-module.*

Proof. The finiteness follows from $\mathrm{Gal}(M_\infty/F_\infty)<\infty$. Let $F^{\mathrm{t.r.}}_{\infty,\mathfrak{p}}$ denote the maximal totally ramified abelian p-extension of $F_{\infty,\mathfrak{p}}$. By local class field theory, we get an isomorphism $\mathrm{Gal}(F^{\mathrm{t.r.}}_{\infty,\mathfrak{p}}/F_{\infty,\mathfrak{p}})\simeq \mathcal{U}^{(1)}_{\mathfrak{p},\infty}=\varprojlim \mathcal{U}^{(1)}_{\mathfrak{p},m}$, where $\mathcal{U}^{(1)}_{\mathfrak{p},m}$ denotes the group of principal units of the completion of F_m for the prime ideal above $\mathfrak{p}$. Let $F_\infty^{\omega\chi_D^{-1}}$ be as in Section 2.1. Since Δ acts on $\mathrm{Gal}(M_\infty/F_\infty)$ via $\omega\chi^{-1}$, we see $F_\infty\subset M_\infty\subset F_\infty^{\omega\chi_D^{-1}}$. By the arguments in Section 2.1, the decomposition group of prime divisor above $\mathfrak{p}$ in $\mathrm{Gal}(M_\infty/F_\infty)$ coincides with the inertia group. Hence, $M_{\infty,\mathfrak{p}}/F_{\infty,\mathfrak{p}}$ is a totally ramified extension and D acts on $\mathrm{Gal}(M_{\infty,\mathfrak{p}}/F_{\infty,\mathfrak{p}})$ via $\omega\chi_D^{-1}$. We have a surjection of $\Lambda_\chi=\mathcal{O}_\chi[[\Gamma]]$-modules

$$(\mathcal{U}^{(1)}_{\mathfrak{p},\infty})_{\omega\chi_D^{-1}}\otimes_{\mathcal{O}_{\chi_D}}\mathcal{O}_\chi\to\mathrm{Gal}(M_{\infty,\mathfrak{p}}/F_{\infty,\mathfrak{p}})\otimes_{\mathcal{O}_{\chi_D}}\mathcal{O}_\chi. \tag{4.3.1}$$

From our assumption $\chi(p)\neq 1$, we know that $(\mathcal{U}^{(1)}_{\mathfrak{p},\infty})_{\omega\chi_D^{-1}}\otimes_{\mathcal{O}_{\chi_D}}\mathcal{O}_\chi$ is isomorphic to Λ_χ [3, Proposition 1]. On the other hand, Γ acts on $\mathrm{Gal}(M_\infty/F_\infty)$ via the cyclotomic character κ, because of the Kummer pairing

$$\mathrm{Gal}(M_\infty/F_\infty)\times W_{F,\chi}\to\mu_{p^\infty}\otimes_{\mathbb{Z}_p}\mathcal{O}_\chi,$$

and $W_{F,\chi}\subset(F^\times\otimes_{\mathbb{Z}}\mathbb{Q}_p/\mathbb{Z}_p)_\chi$. Hence from (4.3.1), we have the surjection of Λ_χ-modules:

$$\Lambda_\chi/(\gamma-\kappa(\gamma))\Lambda_\chi\to\mathrm{Gal}(M_{\infty,\mathfrak{p}}/F_{\infty,\mathfrak{p}})\otimes_{\mathcal{O}_{\chi_D}}\mathcal{O}_\chi.$$

By the isomorphism $\Lambda_\chi/(\gamma-\kappa(\gamma))\Lambda_\chi\simeq\mathcal{O}_\chi$, $\mathrm{Gal}(M_{\infty,\mathfrak{p}}/F_{\infty,\mathfrak{p}})\otimes_{\mathcal{O}_{\chi_D}}\mathcal{O}_\chi$ is a cyclic $\mathcal{O}_\chi$-module, and hence $\mathrm{Gal}(M_{\infty,\mathfrak{p}}/F_{\infty,\mathfrak{p}})$ is a cyclic $\mathcal{O}_{\chi_D}$-module. □

For each $n\in\mathsf{S}$ and each prime ideal $\mathfrak{r}$ of F lying above a rational prime $r\equiv 1\pmod{nN_F}$, let $\beta_{\mathfrak{r},n}$ be the element of $M^\times_{\infty,n}$ which is defined in Section 4.1. Fix a prime ideal $\mathfrak{p}$ of F lying above p, and let $M_{\infty,n,\mathfrak{p}}$ denote the completion of $M_{\infty,n}$ for a prime divisor lying above $\mathfrak{p}$.

Let $g_{\mathfrak{r}}(n)\in\mathbb{Z}$ be the largest power of p which satisfies $\beta_{\mathfrak{r},n}\in(M^\times_{\infty,n,\mathfrak{p}})^{g_{\mathfrak{r}}(n)}$, and define $g(n)=\min\{g_{\mathfrak{r}}(n)\mid \mathfrak{r}\text{: prime ideals of } F \text{ lying above a rational prime } r\equiv 1\pmod{nN_F}\}$.

Remark. We can easily see that the integer $g(n)$ does not depend on a prime divisor of $M_{\infty,n}$ lying above p.

Proposition 3. *Let* $n\in\mathsf{S}$.

$$d(n)^f/[M_\infty : M_{\infty,n}L_{\infty,0}]=\min\{g(n),d(n)\}^f.$$

Proof. Recall the Kummer pairing in Section 4.1:

$$\mathrm{Gal}(M_\infty/M_{\infty,n}) \times W(n) \to \mu_{p^\infty} \otimes_{\mathbb{Z}_p} \mathcal{O}_\chi.$$

By Lemma 10, we can write

$$W(n) = \bigoplus_{i=1}^{k} \mathcal{O}_{\chi_D}/p^{m_i},$$

$$\mathcal{O}_{\chi_D}/p^{m_i} \simeq \langle \beta_{\mathfrak{r}_i,n} \otimes 1/d(n) \rangle_{\mathcal{O}_{\chi_D}},$$

with prime ideals $\mathfrak{r}_i$ of F lying above a rational prime $r_i \equiv 1 \pmod{nN_F}$.

For every i with $1 \leqslant i \leqslant k$, let $K_i = M_{\infty,n}(\{a^{1/p^m} \mid a \otimes 1/p^m \in \langle \beta_{\mathfrak{r}_i,n} \otimes 1/d(n) \rangle_{\mathcal{O}_{\chi_D}}\})$. Then M_∞ is the composite field of all K_i, $1 \leqslant i \leqslant k$.

For a fixed prime ideal $\mathfrak{p}$ of F, let $M_{\infty,n,\mathfrak{p}}$, $K_{i,\mathfrak{p}}$ and $M_{\infty,\mathfrak{p}}$ be the completions of the extensions at a prime divisor lying above $\mathfrak{p}$. Clearly, $K_{i,\mathfrak{p}} = M_{\infty,n,\mathfrak{p}}(\{a^{1/p^m} \mid a \otimes 1/p^m \in \langle \beta_{\mathfrak{r}_i,n} \otimes 1/d(n) \rangle_{\mathcal{O}_{\chi_D}}\})$ and $M_{\infty,\mathfrak{p}}$ is the composite of all $K_{i,\mathfrak{p}}$, $1 \leqslant i \leqslant k$.

For any prime ideal $\mathfrak{r}$ of F lying above a rational prime $r \equiv 1 \pmod{nN_F}$, we have $\beta_{\mathfrak{r},n} \otimes 1/d(n) \in W(n)$ by Lemma 10. Since $W(n)$ is generated by all $\beta_{\mathfrak{r}_i,n} \otimes 1/d(n)$ with $1 \leqslant i \leqslant k$, we get $g_{\mathfrak{r}}(n) \geqslant \min\{g_{\mathfrak{r}_i}(n), d(n) \mid 1 \leqslant i \leqslant k\}$ by Lemma 4(2). Hence we get

$$\min\{g(n), d(n)\} = \min\{g_{\mathfrak{r}_i}(n), d(n) \mid 1 \leqslant i \leqslant k\}.$$

By Lemma 11, $\mathrm{Gal}(M_{\infty,\mathfrak{p}}/M_{\infty,n,\mathfrak{p}})$ is a cyclic $\mathcal{O}_{\chi_D}$-module. Hence we get

$$[M_{\infty,\mathfrak{p}} : M_{\infty,n,\mathfrak{p}}] = \max\{[(K_i)_{\mathfrak{p}} : (M_{\infty,n})_{\mathfrak{p}}] \mid 1 \leqslant i \leqslant k\}.$$

(1) *Case* $d(n) \leqslant g_{\mathfrak{r}_i}(n)$ *for all* i *such that* $0 \leqslant i \leqslant k$. In this case, we have $K_{i,\mathfrak{p}} = M_{\infty,n,\mathfrak{p}}$ for all i. Hence we get $M_{\infty,\mathfrak{p}} = M_{\infty,n,\mathfrak{p}}$. Since $\mathrm{Gal}(M_\infty/M_{\infty,n}L_{\infty,0})$ is generated by decomposition groups in $\mathrm{Gal}(M_\infty/M_{\infty,n})$ of prime divisors above p, we have $[M_\infty : M_{\infty,n}L_{\infty,0}] = 1$, and then we complete the proof in this case.

(2) *Case* $d(n) > g_{\mathfrak{r}_i}(n)$ *for some* i. Let i_0 be such that $g_{\mathfrak{r}_{i_0}}(n) = \min\{g_{\mathfrak{r}_i}(n) \mid 1 \leqslant i \leqslant k\}$. We have by Lemma 4(2)

$$\begin{aligned}\mathrm{Gal}((M_\infty)_{\mathfrak{p}}/(M_{\infty,n})_{\mathfrak{p}}) &= \mathrm{Gal}((K_{i_0})_{\mathfrak{p}}/(M_{\infty,n})_{\mathfrak{p}} \\ &\simeq \mathcal{O}_{\chi_D}/(d(n)/g_{\mathfrak{r}_{i_0}}(n))\end{aligned}$$

and

$$\mathrm{Gal}(M_\infty/M_{\infty,n}L_{\infty,0}) \simeq \mathcal{O}_\chi/(d(n)/g_{\mathfrak{r}_{i_0}}(n)).$$

Hence it follows that $[M_\infty : M_{\infty,n}L_{\infty,0}] = (d(n)/g_{\mathfrak{r}_{i_0}}(n))^f$, and the proof if complete. □

4.4. Let J_F be the idèle group of F, and $\overline{F^\times \prod_{v\nmid p} \mathcal{U}_v}$ be the closure of $F^\times \prod_{v\nmid p} \mathcal{U}_v$ in J_F where $\mathcal{U}_v$ is the group of units of F_v (for an infinite prime divisor, $\mathcal{U}_v$ is defined to be the multiplicative group of F_v). Let $Y_F = J_F/\overline{F^\times \prod_{v\nmid p} \mathcal{U}_v}$ and $Y_F\{p\}$ denotes the p-primary component of Y_F. By class field theory, we have the following exact sequence.

$$0 \to \mathcal{U}^{(1)}/\overline{\mathcal{U}^{(1)} \cap E_F} \to Y_F\{p\} \to A_F \to 0,$$

where $\mathcal{U}^{(1)} = \prod_{\mathfrak{p}|p} \mathcal{U}_\mathfrak{p}^{(1)}$, $\mathcal{U}_\mathfrak{p}^{(1)}$ is the group of principal units of $F_\mathfrak{p}$, and E_F is the group of units of F. By taking the χ-part of the above exact sequence, we get the isomorphism $A_{F,\chi} \simeq Y_F\{p\}_\chi/\mathcal{U}_\chi^{(1)}$. Let $d \in \mathbb{Z} > 0$ be as before, that is, $d^f = |A_{F,\chi}|$ and $\bar{e}_\chi \in \mathbb{Z}[\Delta]$ such that $\bar{e}_\chi \equiv e_\chi \pmod d$. Since $dA_{F,\chi} = 0$, we have

$$(\mathcal{U}_\chi^{(1)})^d \subset d(Y_F\{p\}_\chi) \subset \mathcal{U}_\chi^{(1)}.$$

By the assumption $\omega\chi^{-1}(p) \neq 1$, we have $\mathcal{U}_\chi^{(1)} \simeq \mathcal{O}_\chi$ [3, Proposition 1]. Let v be the order of the residue field of a prime ideal of F lying above p, and $\mathfrak{r}$ a prime ideal of F lying above a rational prime $r \equiv 1 \pmod{N_F}$. By the natural injection $F^\times \hookrightarrow \prod_{\mathfrak{p}|p} F_\mathfrak{p}^\times$, we can regard $(\tau_\mathfrak{r}^{\bar{e}_\chi})^{v-1}$ as an element of $\mathcal{U}^{(1)} = \prod_{\mathfrak{p}|p} \mathcal{U}_\mathfrak{p}^{(1)}$. For any integer $k > 0$, we see

$$d(Y_F\{p\}_\chi) = \langle \{(\tau_\mathfrak{r}^{\bar{e}_\chi})^{v-1} \mid \mathfrak{r}\text{: prime ideals of } F \text{ lying above a rational prime } r \equiv 1 \pmod{kN_F}\} \rangle_{\mathbb{Z}_p}, \tag{4.4.1}$$

(cf. [4, Lemma 4.4]).

Lemma 12. *For any integer $k > 0$, there exists a prime ideal $\mathfrak{r}$ of F lying above a rational prime $r \equiv 1 \pmod{kN_F}$ such that $g_\mathfrak{r}(1) \leqslant d$.*

Proof. For $m \geqslant 0$ we put $\Gamma_m = \mathrm{Gal}(F_m/F)$. By the spectral sequence, we have an exact sequence

$$0 \to H^1(\Gamma_m, \bigoplus_{\mathfrak{p}|p} \mu_{p^m}(F_{m,\mathfrak{p}})) \to \bigoplus_{\mathfrak{p}|p} F_\mathfrak{p}^\times/(F_\mathfrak{p}^\times)^{p^m} \to (\bigoplus_{\mathfrak{p}|p} F_{m,\mathfrak{p}}^\times/(F_{m,\mathfrak{p}}^\times)^{p^m})^{\Gamma_m}$$
$$\to H^2(\Gamma_m, \bigoplus_{\mathfrak{p}|p} \mu_{p^m}(F_{m,\mathfrak{p}})) \to \cdots.$$

By taking the χ-part of the above exact sequence, we get

$$\left(\bigoplus_{\mathfrak{p}|p} F_\mathfrak{p}^\times/(F_\mathfrak{p}^\times)^{p^m}\right)_\chi \simeq \left\{\left(\bigoplus_{\mathfrak{p}|p} F_{m,\mathfrak{p}}^\times/(F_{m,\mathfrak{p}}^\times)^{p^m}\right)^{\Gamma_m}\right\}_\chi, \tag{4.4.2}$$

because of $(\oplus_{\mathfrak{p}|p}\mu_{p^m}(F_{m,\mathfrak{p}}))_\chi = 0$ from $\omega\chi^{-1}(p)\neq 1$ [3, Proposition 1]. The assertion follows this and (4.4.1). □

We write as in Section 4.2,

$$V_\chi^\Gamma = \bigoplus_{i=1}^{t} \mathcal{O}_\chi/p^{e^i}, \quad e_1 \geqslant \cdots \geqslant e_t,$$

$$\mathcal{O}_\chi/p^{e_i} \simeq \langle a_i \otimes 1/p^{m_i} \rangle_{\mathcal{O}_\chi}, \quad (a_i \otimes 1/p^{m_i} \in (F^\times \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p)_\chi).$$

Proof of Theorem 2. Let $n \in \mathsf{S}_i$, $0 \leqslant i \leqslant t$. We can easily see from (4.1.2) that

$$\begin{aligned} |V_\chi^\Gamma/T(n)\cap V_\chi^\Gamma| &= [L_{\infty,0} : M_{\infty,n}\cap L_{\infty,0}] \\ &= [M_{\infty,n}L_{\infty,0} : M_{\infty,n}] \\ &= [M_\infty : M_{\infty,n}]/[M_\infty : M_{\infty,n}L_{\infty,0}] \\ &= |W(n)|/[M_\infty : M_{\infty,n}L_{\infty,0}]. \end{aligned}$$

From this and Proposition 3, we get

$$\begin{aligned} |V_\chi^\Gamma/T(n)\cap V_\chi^\Gamma| \times d(n)^f/|W(n)| &= d(n)^f/[M_\infty : M_{\infty,n}L_{\infty,0}] \\ &= \min\{g(n), d(n)\}^f. \end{aligned} \tag{4.4.3}$$

Note that $d(n)^f/|W(n)| \geqslant 1$ from (3.2.5).

We can choose $n_i \in \mathsf{S}_i$ from Proposition 2 which satisfies

$$T(n_i) = \bigoplus_{j=1}^{i} \langle a_j \otimes 1/p^{m_j} \rangle_{\mathcal{O}_\chi}$$

and

$$|W(n_i)| = d(n_i)^f.$$

Hence we have

$$\begin{aligned} \min\{|V_\chi^\Gamma/T(n)\cap V_\chi^\Gamma| \mid n \in \mathsf{S}_i\} &= |V_\chi^\Gamma/T(n_i)| \\ &= p^{(e_{i+1}+\cdots+e_t)f}. \end{aligned}$$

Further, since $|W(n_i)| = d(n_i)^f$ we have

$$\min\{|V_\chi^\Gamma/T(n)\cap V_\chi^\Gamma| \times d(n)^f/|W(n)| \mid n \in \mathsf{S}_i\} = p^{(e_{i+1}+\cdots+e_t)f}.$$

From (4.4.3), we get

$$\min\{g(n), d(n) \mid n \in \mathsf{S}_i\} = p^{e_{i+1}+\cdots+e_t}. \tag{4.4.4}$$

On the other hand, we have $F_{\infty,\mathfrak{p}} = M_{\infty,n_i,\mathfrak{p}}$ for every prime ideal $\mathfrak{p}$ of F lying above p because $F_\infty \subset M_{\infty,n_i} \subset L_{\infty,0}$ and $\mathfrak{p}$ is totally decomposed in $L_{\infty,0}/F_\infty$. By Lemma 12, there exists a prime ideal $\mathfrak{r}$ of F lying above a rational prime $r \equiv 1 \pmod{n_i N_F}$ such that $g_\mathfrak{r}(1) \leqslant d$. By the definition, $\beta_{\mathfrak{r},n_i} = \beta_{\mathfrak{r},1}^{d(n_i)/d}$ is an element of $M_{\infty,n_i}^\times$ and $g_\mathfrak{r}(n_i)$ is the largest power of p satisfying $\beta_{\mathfrak{r},n_i} \in (M_{\infty,n,\mathfrak{p}}^\times)^{g_\mathfrak{r}(n_i)} = (F_{\infty,\mathfrak{p}}^\times)^{g_\mathfrak{r}(n_i)}$. Hence we get from $g_\mathfrak{r}(1) \leqslant d$ that

$$\begin{aligned} g_\mathfrak{r}(n_i) &= g_\mathfrak{r}(1) \times d(n_i)/d \\ &\leqslant d(n_i). \end{aligned}$$

It concludes from this that

$$\begin{aligned} \min\{g(n), d(n) \mid n \in \mathsf{S}_i\} &= \min\{g(n_i), d(n_i)\} \\ &= g(n_i) \\ &= \min\{g(n) \mid n \in \mathsf{S}_i\}, \end{aligned}$$

and using (4.4.4), we complete the proof. □

Proof of Corollary 2. It is sufficient to show the isomorphism $X_{\omega\chi^{-1}}/(\gamma - \kappa(\gamma))X_{\omega\chi^{-1}} \simeq \mathscr{T}_\chi$. Since we assumed $\omega\chi^{-1}(p) \neq 1$, this follows from the isomorphism

$$\mathscr{T}_\chi \simeq \mathrm{Hom}_{\mathscr{O}_\chi}(X_{\omega\chi^{-1}}/(\gamma - \kappa(\gamma))X_{\omega\chi^{-1}}, \mu_{p^\infty} \otimes_{\mathbb{Z}_p} \mathscr{O}_\chi)$$

(cf. [8]). □

Proof of Corollary 3. Let D be the decomposition group of p in $\Delta = \mathrm{Gal}(F/\mathbb{Q})$, and χ_D the restriction of χ to D. Since $\mathscr{W}_\chi^{(1)} \simeq (\mathscr{W}_\mathfrak{p}^{(1)})_{\chi_D} \otimes_{\mathscr{O}_{\chi_D}} \mathscr{O}_\chi$ and (4.4.2), we get the conclusion. □

Acknowledgments

I thank the thesis advisor Professor M. Kurihara for valuable discussions and advice.

References

[1] M. Aoki, The Iwasawa main conjecture and Gauss sums, J. Number Theory 89 (2001) 151–164.
[2] M. Aoki, Notes on the structure of the ideal class groups of abelian number fields, submitted.
[3] R. Gillard, Unités cyclotomiques, unités semi-locales et $\mathbb{Z}_\ell$-extensions II, Ann. Inst. Fourier 29 (4) (1979) 1–15.
[4] Y. Hachimori, H. Ichimura, Semi-local units modulo Gauss sums, Manuscripta Math. 95 (1998) 377–395.
[5] K. Iwasawa, A note on Jacobi sums, Symp. Math. XV (1975) 447–459.
[6] V. Kolyvagin, Euler systems, in the Grothendieck Festschrift II, Progr. Math. 87 (1990) 435–483.
[7] B. Mazur, A. Wiles, Class fields of abelian extensions of $\mathbb{Q}$, Invent. Math. 76 (1984) 179–330.
[8] T. Nguyen Quang Do, Sur la $\mathbb{Z}_p$-torsion de certains modules galoisiens, Ann. Inst. Fourier 36 (1986) 27–46.
[9] K. Rubin, Kolyvagin's system of Gauss sums, in Arithmetic Algebraic Geometry, Progr. Math. 89 (1991) 309–324.
[10] L. Washington, Introduction to cyclotomic fields, Graduate Texts in Mathematics, 2nd Edition, Vol. 83, Springer, Berlin, New York, 1997.